

Sealed
Public and unofficial staff access
to this instrument are
prohibited by court order

United States Courts
Southern District of Texas
FILED

AO 91 (Rev. 11/11) Criminal Complaint

April 09, 2022

UNITED STATES DISTRICT COURT

for the

Nathan Ochsner, Clerk of Court

Southern District of Texas



United States of America
v.
MARCOS TREVINO

Case No.

4:22-mj-819

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of from June 30, 2018 to April 8, 2022 in the county of Brazos and Grimes in the
Southern District of Texas, the defendant(s) violated:

Code Section

18 USC 1953
18 USC 1343
18 USC 1349

Offense Description

Interstate Transportaiton of Wagering Paraphernalia
Wire Fraud
Conspiracy to Commit Wire Fraud

This criminal complaint is based on these facts:
See attached affidavit

☒ Continued on the attached sheet.



Complainant's signature

FBI SA Jared Harshbarger

Printed name and title

Sworn to before me and signed telephonically.

Date: 04/09/2022

City and state: Houston, Texas



Judge's signature
Hon. Yvonne Y. Ho., U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND SEARCH AND SEIZURE WARRANTS

1. I, Jared Harshbarger, Special Agent of the Federal Bureau of Investigation (FBI), having been duly sworn, depose and state as follows:

Introduction

2. I am submitting this affidavit in support of **(1) a criminal complaint and arrest warrant against Marcos Trevino (“Trevino”); (2) an application for seizure warrant for the funds not to exceed \$80,325 contained in Wells Fargo checking account number 2019920107 held in the name of Marcos Trevino (“Target Account” or account “0107”); (3) an application for a seizure warrant for a 2018 Dodge Demon, VIN: 2C3CDZH98JH102818 held in the name of Marcos Trevino. (“Target Vehicle”); and (4) a search warrant for the residence located at 9418 Lancaster Drive, Iola, TX, 77861 (“Target Property”) (Attachment A) and the items located therein as described in Attachment B.**

3. I am a Special Agent with FBI, and a Federal law enforcement officer within the meaning of Rule 41(h), Federal Rules of Criminal Procedure. I am authorized by Rule 41(a), Federal Rules of Criminal Procedure to make application for search and seizure warrants and to serve arrest warrants pursuant to Rule 4(a) and (d)(1), Federal Rules of Criminal Procedure. I am a Special Agent with the FBI and have been since June 2021. I am currently assigned to the Houston, Texas Division of the FBI, Bryan Resident Agency, where I conduct a variety of investigations dealing with criminal violations. I received law enforcement training at the FBI Academy in Quantico, Virginia. Portions of my duties are dedicated to investigating cases involving an assortment of crimes including fraud and money laundering. Since becoming a Special Agent, I work with experienced Special Agents who also investigate a myriad of criminal violations to include wire fraud and money laundering.

4. The statements in this affidavit are based on my personal knowledge, information I have received from other law enforcement personnel, and from other individuals with knowledge of relevant facts. The statements in this affidavit are also based upon information I received from reviewing documents and other records relevant to the investigation, such as bank account records. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

5. I have set forth facts that I believe are sufficient to establish probable cause to believe that Marcos Trevino has committed the offenses of 18 USC § 1953 (Interstate Transportation of Wagering Paraphernalia), 18 USC § 1343 (Wire Fraud), and 18 USC § 1349 (Conspiracy to Commit Wire Fraud) (hereinafter referred to as the “Subject Offenses”).

6. In addition, I have set forth facts that I believe are sufficient to establish probable cause that the **Target Vehicle** and funds in the **Target Account** constitute evidence, instrumentalities, property used and designed for use, and fruits of violation of 18 USC § 1953 (Interstate Transportation of Wagering Paraphernalia), 18 USC § 1343 (Wire Fraud), and, 18 USC § 1349 (Conspiracy to Commit Wire Fraud), are that such funds in the **Target Account**, as well as the **Target Vehicle**, represent property which constitute and were derived from proceeds traceable to violations of 18 USC § 1953, 18 USC § 1343, and 18 USC § 1349, and are thus subject to seizure pursuant to Federal Rule of Criminal Procedure 41 and subject to forfeiture pursuant to 18 USC § 981(a)(1)(D)-(E) and 18 USC § 982(a)(2)-(4).

7. In addition, I have set forth facts that I believe are sufficient to establish probable cause that the funds in the **Target Account** as well as the **Target Vehicle** would, in the event of conviction, be subject to forfeiture and that an order under 18 USC § 981(a)(1)(D)-(E), 18 USC §

982(a)(2)-(4), and 18 USC § 983 may not be sufficient to assure the availability of the property for forfeiture.

8. In addition, I have set forth facts that I believe are sufficient to establish probable cause that the items listed in Attachment B that are contained in Attachment A (the Target Property) constitute evidence, instrumentalities, property used and designed for use, and fruits of violation of 18 USC § 1953 (Interstate Transportation of Wagering Paraphernalia), 18 USC § 1343 (Wire Fraud), and, 18 USC § 1349 (Conspiracy to Commit Wire Fraud).

Relevant State Law

9. Pursuant to Chapter 47.03 of the Texas Penal Code, Gambling Promotion, it is a Class A misdemeanor if a person intentionally or knowingly operates or participates in the earnings of a gambling place, engages in bookmaking, or for gain becomes a custodian of anything of value bet or offered to be bet.

10. Chapter 47.06 of the Texas Penal Code, Possession of Gambling Device, Equipment, or Paraphernalia, makes it a Class A misdemeanor if a person, with the intent to further gambling, knowingly owns, manufactures, transfers, or possesses any gambling device that he knows is designed for gambling purposes or any equipment that he knows is designed as a subassembly or essential part of a gambling device.

11. The Texas Penal Code defines “gambling device” as any electronic, electromechanical, or mechanical contrivance that for consideration affords the player an opportunity to obtain anything of value, the award of which is determined solely or partially by chance, even though accompanied by some skill, whether or not the prize is automatically paid by the contrivance. The term further includes, but is not limited to, gambling device versions of bingo, keno, blackjack, lottery, roulette, video poker, or similar electronic, electromechanical, or

mechanical games, or facsimiles thereof, that operation by chance or partially so, that as a result of the play or operation of the game award credits or free games, and that record the number of free games or credits so awarded and the cancellation or removal of the free games or credits. The definition specifically excludes any electric, electromechanical, or mechanical contrivance designed, made, and adapted solely for bona fide amusement purposes if the contrivance rewards the player exclusively with noncash merchandise prizes, toys, or novelties, or a representation of value redeemable for those items, that have a wholesale value available from a single play of the game or device of not more than 10 times the amount charged to play the game or device once or \$5, whichever is less.

12. Importantly, it is a defense to these offenses if the gambling operation is authorized under Chapter 2002 of the Texas Occupations Code. *See* Texas Penal Code §§ 47.02(c)(2), 47.09(a)(1)(B). That Chapter governs raffles in the State of Texas

13. Texas Occupations Code § 2002.052(d)-(f) states that “[b]efore settling of offering to sell tickets for a raffle, a qualified organization **shall set a date** on which the organization will award the prize or prizes in a raffle. The organization must award the prize or prizes on that date unless the organization becomes unable to aware the prize or prizes on that date. A qualified organization that is unable to award a prize or prizes on the date set . . . **may set another date not later than 30 days from the date originally set** on which the organization will award the prize or prizes. If the prize or prizes are not awarded within the 30 days, . . . the organization **must refund or offer to refund** the amount paid by each person who purchased a ticket for the raffle” (emphasis added).

14. Moreover, a raffle can only be conducted by a qualified organization, which is defined as a qualified religious society, qualified volunteer fire department, qualified volunteer

emergency medical service, or qualified nonprofit organization.” Texas Occupations Code § 2002.02(2) and 2002.051.

15. In addition, “[a]ll proceeds from the sale of tickets for a raffle must be spent for the charitable purposes of the qualified organization.” Texas Occupations Code § 2002.053.

16. Also, a raffle may not: “(a) directly or indirectly, by the use of paid advertising, promote a raffle through a medium of mass communication, including television, radio, or newspaper; (b) promote or advertise a raffle statewide, other than on the [qualified] organization's Internet website or through a publication or solicitation, including a newsletter, social media, or electronic mail, provided only to previously identified supporters of the [qualified] organization; or (c) sell or offer to sell tickets for a raffle statewide.” Texas Occupations Code § 2002.054.

17. Therefore, a raffle can only be lawful in Texas if it is conducted by a qualifying non-profit corporation, it is conducted on a set date and can only be continued for 30 days, the amount participants spend is refunded if the prize is not awarded within 30 days of the last date set, the proceeds are spent on a charitable purpose of the qualifying organization, and the raffle is not advertised on a statewide basis.

Background:

18. Marcos Trevino (hereinafter Trevino) is a self-identified entrepreneur engaged in wire fraud activities and the promotion of fraudulent (illegal) raffle(s) who is reportedly employed by Hunter Pharmacy Services and reported his income to be \$150,000.00. The raffle(s) he promotes offers a chance to win limited edition Dodge Challenger(s) SRT Demon automobile(s). Beginning in 2018, and continuing through today, Trevino has promoted such a raffle via various media platforms to include a link to a raffle via <http://www.thecapitalisthustler.com>, Facebook, and in person at various auto shows.

19. The raffle(s) appears to have been initiated on or about June 30, 2018 and was set to end on July 4, 2019 (or sooner), and Trevino calls it the “2018 Dodge Demon Sweepstakes Giveaway.” This raffle was to occur if all 2,000 tickets were sold. On the raffle site under the RULES AND REGULATIONS page was a listed a start date of July 31, 2018 with no end date (which, as previously stated, is in violation of Texas law). It was also stated the raffle will be held after 2,000 tickets were sold, or immediately if all 3,300 tickets were sold. The Brazos County Sheriff's Department reported that on or about January 4, 2020, the raffle site reported 597 tickets had been sold.

20. According to the Brazos County Sheriff's Department, the raffle website makes it appear as though the participant is not purchasing a ticket, but rather a BCS Mopar Club "Koozie" (i.e., a foam beverage holder), which, in turn, will grant the participant one entry for the drawing. The koozies are \$100 each plus a \$5 processing fee (in other words, \$105 for a foam beverage holder). The RULES AND REGULATIONS page also explicitly state, "NO PURCHASE NECESSARY TO ENTER OR WIN. A PURCHASE WILL NOT IMPROVE YOUR CHANCE OF WINNING." However, aside from the purchase of the koozie for a total of \$105, there is no alternate means of entry. In addition, although the website claims that “MONEY BACK GUARANTEED,” the Rules and Regulations state that “[r]efund per customer request within 30 days of original purchase date, after such date not valid for refund.” Not only is there no method described for a participant to get his/her money back, but as explained above, such terms are in violation of Texas law.

21. On January 10, 2020, Brazos County investigators started an investigation into Trevino and the alleged illegal gambling activity in violation of Texas Penal Code violation 47.03 Gambling Promotion 39B - Operating/Promoting/Assisting Gambling 47.03/39990001. Brazos

County Sheriff's Department Investigators contacted Trevino via cell phone. Brazos County Investigators reported Trevino informed them the raffle would take place when all 2,000 koozies were sold, and if 2,000 koozies didn't sell, Trevino would likely give another car away as a prize of lesser value. Investigators asked Trevino if he was affiliated with a nonprofit organization or charity to which Trevino informed investigators he was not. Trevino informed investigators he planned to donate a percentage of the money to the Humane Society and a local breast cancer society. However, he was unable to provide the name of either entity. Trevino told investigators multiple times that he spoke to a lawyer out of Houston regarding running a raffle. However, Trevino could not provide a name of said lawyer.

22. On August 31, 2020, Trevino was arrested on a Brazos County warrant at his residence by the Grimes County Sheriff's Department. The case has yet to be adjudicated. Even after being arrested, Trevino's website for the raffle continued to operate and is still operational. According to the website, total ticket sales have reached 765 (which, at \$105 per ticket, would be a total of \$80,325, and at \$100 per ticket, would be a total of \$76,500). The identity of those who have entered is limited to the person's first name and last initial. Trevino is continuing to conduct illegal raffles in the State of Texas and utilizing the service PayPal to collect the \$105 entry fees. PayPal, which is based in San Jose, California (outside of the State of Texas), is used by Trevino as a mechanism to process transactions for the raffle(s).

23. Despite the raffle being in existence for almost four years, there has been no drawing or receipt of prizes by any participants. Meanwhile, Trevino has amassed over \$75,000 from the scheme.

24. As explained above, the raffles are illegal for Trevino to conduct in the State of Texas because they are not run by a charitable organization, a date certain was not set, the amount

was not refunded in the required time, the proceeds were not spent on a lawful purpose, and there was statewide advertising. Indeed, to date, which is almost four years after the raffle began, no raffle has been conducted, nor has there been a winning recipient. Moreover, at present, law enforcement is unaware of any participant receiving a koozie or a refund.

Interview of Victims:

25. Victim 1 (V1) participated in the 2018 Dodge Demon – Sweepstakes Giveaway. V1 described the car as a plum purple Dodge Demon. The Vehicle Identification Number (VIN) for the car being raffled ended in 2818, which is the same as the **Target Vehicle**. V1 purchased one ticket for \$100 via PayPal. V1 and did not receive a koozie as advertised. V1 did not try to receive a refund and did not receive any correspondences from the raffle coordinator. V1 shared with law enforcement a post on Facebook, promoting the raffle in hopes that the minimum 2,000 tickets would be sold, and the car would be raffled. V1 was contacted on April 29, 2019, by a friend on Facebook, who said “Don’t bother on that giveaway. They have been doing this car for a year or two now.” When purchasing a ticket and a chance to win the Dodge Demon, V1 indicated that each individual could choose their own ticket number.

26. Victim 2 (V2) was telephonically informed about the raffle by *Joy Trevino (Marcos Trevino’s wife)*, who was his/her friend. V2 provided Marcos Trevino \$100 in person. However, he/she has never received anything in return (including a koozie). About one to one and one-half years ago, V2 talked with Trevino and Trevino stated the car would not be raffled off until further notice due to pending criminal actions against him. V2 was not aware that anyone has ever won the Purple Dodge Demon or anything similar in relation to this raffle. V2 did not request a refund for the \$100. V2 also stated that Trevino goes by the alias “The Capitalist Hustler” and under that name he goes to different car shows in the Bryan/College Station area promoting the raffle.

27. Victim 3 (V3) found out about a Dodge Demon being raffled after spotting it at a car event called "Lucky's (sp) Rod Run." The car event was annually held at the beginning of January. V3 believed that the event in question took place a few years ago, possibly in 2018. V3 recounted that the purple Dodge Demon was on a trailer. V3 inquired about the car while at the event but did not purchase a ticket to the raffle until later. V3 bought one ticket for the raffle and paid for it online. The Raffle owner, whose name V3 could not recall, updated the status of the drawing using the social media platform Facebook. The owner of the raffle event continuously extended the raffle. The raffle owner also sent emails to V3 requesting V3 buy more tickets. V3 never tried to get his/her money back because he/she believed that someone else had won the Dodge Demon. V3 believed that the Raffle owner had been to other car events. V3 believed this was the only car being raffled and there was never a mention of any other car to be raffled in its place. V3 provided a receipt for the purchase of the raffle ticket. V3 never received a koozie or anything of value.

28. V1, V2, and V3 were never informed that the raffle conducted by Trevino is illegal under Texas law.

29. In addition, your affiant has researched the residence of other victims (i.e., raffle participants) of Trevino's scheme and determined that several reside outside of the State of Texas.

30. The other over 700 victims are only identified by their first name and last initial on the aforementioned website. Thus, further information from Trevino's records (whether in document form or electronic) is needed to further identify and contact the victims.

Truist Bank Loan

31. Your affiant obtained loan information for the vehicle to be raffled from Truist Bank, which is headquartered in Charlotte, North Carolina. The loan is for a PUVN N 2018 Dodge

Challenger SRT DE, VIN: 2C3CDZH98JH102818, which matches the raffle advertisement. The date of the loan opening is July 28, 2018, which was after the start of the raffle of June 30, 2018. The loan for VIN: 2C3CDZH98JH102818 was paid off on December 22, 2021, after the start of the raffle and after Trevino had begun receiving proceeds from the raffle. The VIN matches that of the **Target Vehicle**.

2018 Dodge Demon Sweepstakes Giveaway – VON/VON:

32. Your affiant contacted the General Manager at Lithia Chrysler Jeep Dodge of Bryan/College Station, in reference to identification of a Vehicle Identification Number (VIN) with an associated Vehicle Order Number (VON).¹ Your affiant provided VON 40106928 which was the advertised VON number for the 2018 Dodge Demon Sweepstakes Giveaway. The Manager returned with VIN 2C3CDZH98JH102818, which is for the **Target Vehicle** and is registered to **Marcos Trevino**. Your affiant has learned through law enforcement investigations that the **Target Vehicle** is believed to be at the **Target Property** referred to in Attachment A.

Associated Persons, Businesses and Organizations

33. Marcos Trevino conducted, financed, managed, supervised, and owned all or parts of said illegal gambling business, and which remained in substantially continuous operation for a period in excess of thirty days (namely, June 30, 2018 to the present).

34. *Joy Trevino (Joy), who is Trevino's wife, directed the sale of raffle tickets* for the 2018 Dodge Demon Sweepstakes Giveaway. Joy informed individuals of the 2018 Dodge Demon Sweepstakes Giveaway. As of September 12, 2011, Joy is listed as a Secondary Owner for the

¹ A VON is a vehicle order number that is assigned to a vehicle while it is being built. A VIN (vehicle identification number) is assigned to the car once it is fully assembled.

Target Account, which has been identified as the primary account receiving funds from PayPal and which contains ill-gotten proceeds from the 2018 Dodge Demon Sweepstakes Giveaway.

35. PayPal was utilized by aiding in the financing throughout the 2018 Dodge Demon Sweepstakes Giveaway by facilitating the sale of chances to win a Dodge Demon. Over the total activity period, \$57,057.46 of the deposits into x0107 came from PayPal. This was the third largest form of income to the account over the summarized financial activity period. Trevino utilized PayPal to facilitate the sale of raffle tickets in the form of purchasing a “BCS Mopar Koozie.” Upon the purchase of a “BCS Mopar Koozie,” recipients would choose their desired Koozie Number and then receive a confirmation email with the following information:

Merchant: Marcos Trevino (hemi666@yahoo.com)

Description:

- BCS Mopar Koozie
- Item #: ____
- Koozies: 1 Koozie
- Full Name: ____
- Phone Number: ____
- Your Desired Koozie Number: ____
- Payment: \$105.00 USD

36. As previously mentioned, at present, law enforcement has no record of any participant actually receiving a koozie.

37. Below are some, but not all, of the PayPal transfers to Trevino’s Wells Fargo Checking x0107 (the **Target Account**):

13-Jun-20	Withdraw Funds to Bank Account	(\$2,000.00)	WELLS FARGO Checking (Confirmed) x-0107
15-Apr-19	Withdraw Funds to Bank Account	(\$2,033.27)	WELLS FARGO Checking (Confirmed) x-0107
01-Jun-19	Withdraw Funds to Bank Account	(\$2,130.49)	WELLS FARGO Checking (Confirmed) x-0107
24-Jan-19	Withdraw Funds to Bank Account	(\$2,238.45)	WELLS FARGO Checking (Confirmed) x-0107
16-May-19	Withdraw Funds to Bank Account	(\$2,338.57)	WELLS FARGO Checking (Confirmed) x-0107
07-Jan-19	Withdraw Funds to Bank Account	(\$2,441.28)	WELLS FARGO Checking (Confirmed) x-0107

08-Jun-19	Withdraw Funds to Bank Account	(\$3,009.45)	WELLS FARGO Checking (Confirmed) x-0107
-----------	-----------------------------------	--------------	---

38. Trevino utilized PayPal in furtherance of his scheme, namely, to receive payments from victims. PayPal is a worldwide payment system that supports online money transfers and served as an electronic alternative to traditional paper methods, such as checks and money orders. PayPal operates as a payment processor for online vendors, auction sites, and many other commercial users, including Ebay, and online auction site. PayPal offers two different types of accounts – personal and business accounts. A personal account is recommended for individuals who shop and pay online. Personal accounts include premier accounts, which are recommended for casual sellers or non-businesses who wish to get paid online and who also make online purchases. A business account is recommended for merchants who operate under a company/group name. A PayPal user could create a PayPal account by entering an email address and password. PayPal then verifies the email address. A PayPal user then registers the account by using personal information, such as a name, address and phone number. PayPal requires the user to provide a social security number under certain circumstances. To open an account, a PayPal user must agree to comply with PayPal's policies, including a User Agreement and Privacy Statement. If a PayPal user wishes to receive or transfer money through PayPal, that user is required to link a bank account to the PayPal account. If the user's bank was one listed on the PayPal registration website, then that PayPal user has the option to enter his/her online banking login information to automatically link the bank account to the PayPal account. If the user's bank was not listed on the PayPal website, the PayPal user has to enter a bank account number and

routing number. PayPal then confirms the bank account by making two small deposits into the account, totaling less than one dollar. The PayPal user needs to enter those two values in order to confirm the identity of user as the owner or as one with authority to use that bank account. PayPal can also be used to manage credit cards, debit cards, and prepaid gift cards, allowing the user to checkout from websites without having to enter the card information each time. The PayPal user links the card number, expiration date, and security code to the PayPal account. PayPal requires that the name of the card matches the legal name entered when the user created the PayPal account. Uploading documents to PayPal uses facilities of interstate or foreign commerce, and affects such commerce.

39. Wells Fargo of San Francisco, California, and Truist Bank of Charlotte, North Carolina, are federally insured financial institutions in that they are insured depository institutions under the Federal Deposit Insurance Act. Trevino's Wells Fargo account (the **Target Account**) received the proceeds from the raffle through PayPal. Truist Bank funded the automobile loan for the **Target Vehicle** and, based on a review of Trevino's lack of any other regular income, there is probable cause to believe that Trevino partially paid off that loan with proceeds from the raffle.

40. Trevino utilized Facebook page "BCS Mopar" to advertise for the Dodge Demon Sweepstakes Giveaway and direct individuals on how to participate in the raffle. A Facebook post from January 12, 2019, reads as follows, "Things just got a whole lot better! Now when you enter in the Dodge Demon Sweepstakes Giveaway the winning odds are now 1 in 2,000! Drawing to be scheduled on July 4, 2019 or sooner as long as all koozies are sold. Someone is going to win this Demon. Maybe it'll be you!" Trevino utilized Facebook to attract individuals to attend various functions in which they would be able to purchase a Koozie in an attempt to win the Dodge Demon. At the functions, Trevino would accept payments of cash or through PayPal. Facebook is

headquartered in Menlo Park, California, and its website can be accessed in every State and internationally.

41. <http://www.thecapitalisthustler.com> is a website which was utilized to manage the 2018 Dodge Demon Sweepstakes Giveaway hosted by Trevino. Content on the website contained information about the raffle, rules/regulations, vehicle information, and how to pay for a chance to win the Dodge Demon. The website is powered by WordPress, which is a company headquartered in San Francisco, California.

Financial Transaction Activity

42. Linking account x0107 to PayPal: Over the total activity period, \$57,057.46 of the deposits into the **Target Account** came from PayPal. This was the third largest form of income to the account over the summarized financial activity period. The PayPal deposits and transfers help fund personal payments (Loans, phone bills, Sam's Club, & maintenance) for Trevino.

43. Linking account x0107 to raffle: On July 18 and 19, 2018, two deposits were made to x0107 that reference "Koozie." They are:

July 18, 2018 Transfer from Ryan Meyer - \$100.00

a. "Koozie"

July 19, 2018 Transfer from Noble Jack - \$200.00

b. "Koozies"

There are other transfer deposits during 2018 from various individuals for \$100.00, but they do not have a memo. There are 3 deposits to x0107 that reference Demon.

44. Trevino claimed that he planned to donate a percentage of the money to the Humane Society and a local breast cancer society (both entities remained unnamed). Neither of these entity types appear in the withdrawals of this account x0107.

45. Very little funds are retained within the **Target Account** for a long period of time. There appears to be a pattern of quickly moving funds in and out of the **Target Account**. Additionally, there have been \$122,300.00 withdrawn in person at banks from the **Target Account** during the financial review period. Financial analysis indicates there is comingling of proceeds from the 2018 Dodge Demon Sweepstakes Giveaway originating in x0107 and then being spread to additional accounts and cash withdrawals.

Conclusion For Criminal Complaint And Seizure of Target Account and Target Vehicle

46. Based upon the facts and circumstances outlined within this affidavit, your Affiant submits that there is probable cause to believe that Trevino is conducting an illegally gambling operation under Texas law through the use of interstate wires. There is also probable cause to believe that Trevino's gambling operation is an artifice to defraud in that it has been ongoing for almost four years, he has collected over \$76,500 from raffle sales, the vehicle being advertised is still in Trevino's possession, and all individuals identified as purchasers of tickets have not received anything of value. Trevino is also using interstate wires to receive payments, send tickets/receipts and advertise the scheme. Trevino is also defrauding the participants in the raffle as they have received nothing of value (including a koozie or the vehicle) in exchange for sending him \$105 for a ticket.

47. Moreover, based upon the facts and circumstances outlined within this affidavit, your Affiant submits that there is probable cause to believe that the **Target Account** currently holds proceeds from Trevino's criminal activity of violating 18 USC § 1953 (Interstate Transportation of Wagering Paraphernalia), 18 USC § 1343 (Wire Fraud), and 18 USC § 1349 (Conspiracy to Commit Wire Fraud), and that the funds contained in the **Target Account** represent property which constitutes and was derived from proceeds traceable to violations of 18 USC §

1953, 18 USC § 1343, and 18 USC § 1349 and are thus subject to forfeiture pursuant to 18 USC § 981(a)(1)(D)-(E), 18 USC § 982(a)(2)-(4), and 18 USC § 983. There is also probable cause to believe that these proceeds were used, in part, to complete payment of the **Target Vehicle**. Therefore, your Affiant requests the issuance of a Seizure Warrant for the **Target Account and Target Vehicle** described in this affidavit. Further, your affiant submits that there is probable cause to believe that the **Target Account** and **Target Vehicle** would, in the event of a conviction, be subject to forfeiture and that an order issued at that point would be insufficient, absent the issuance of a seizure order, to assure the availability of these items for forfeiture.

48. Similarly, as the entire basis of the scheme forming the basis of Trevino's federal and state offenses is the **Target Vehicle**, there is probable cause to search and seize the **Target Vehicle** as evidence of the crime, fruits of the crime, and property used in committing the crime. *See* Fed. R. Crim. P. 41(c)(1)-(3).

Search Warrant for Target Property

Background Regarding Computers, the Internet, and Email

49. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. This term expressly includes items that fit this definition even if they are not commonly referred to as "computers." Such items include smart phones and tablets. Unless otherwise indicated, "computer" is used interchangeably with "digital device."

50. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs,

and other magnetic or optical media.

51. The terms “information,” “records,” “documents,” “programs,” “applications,” and “materials” include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

52. Based on my training and knowledge and the experience of investigators and other law enforcement personnel assisting in this investigation, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web (“www”) is a functionality of the Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user’s computer, transmitted to the subscriber’s mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

d. Domain name: An identification label (such as www.example.com) that

allows users to easily locate a website. Domain names resolve back to specific IP addresses; thus, for example, www.example.com would resolve back to one IP address. There can be many domain names that resolve back to the same IP address.

e. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Server: A computer, or a series of computer systems, that operates or “hosts” websites and software applications. Unlike a personal computer, a server allows software applications or websites running on it to be accessed by multiple people simultaneously. The term “server” often refers to either the computer hardware itself or the software running on it. For the purposes of this affidavit, I use the term server to refer to a “web” server, which hosts web pages and applications that can be accessed through the Internet.

Items to be Seized are Still Likely in the Place to be Searched

53. Based on my training and experience, I respectfully submit there is probable cause to believe that the place to be searched (Attachment A) still contains the items to be seized (Attachment B).

54. I submit there is probable cause to believe that cell phones, tablets, computers, and other digital devices used by Marcos and/or Joy Trevino (*see* paragraphs 26 and 34 regarding her involvement) may contain names, addresses and phone numbers of co-conspirators and victims, as well as digital evidence such as communications, documents, and similar information with other conspirators and victims. This is particularly true as the victims and/or co-conspirators need a way of communicating with Trevino, who law enforcement investigations revealed, has been running the raffle, in part, from the Target Property (Attachment A).

55. People engaged in the Subject Offense (18 USC §§ 1953, 1343, and 1349) frequently keep records of the acts they did in furtherance of the offense in case they need these records to resolve a dispute between the co-conspirators and/or victims. I know that that these and other records are often retained not just in physical, but electronic form as well.

56. Storing their communications in digital form would make it easier for the potential conspirators to evade detection because a phone or computer outwardly looks less suspicious than physical documents which may bear the victims' information.

57. People who commit the Subject Offense (18 USC §§ 1953, 1343, and 1349) need a place where they can further their illicit activities while minimizing the chance they will be detected. I know based on my training and experience those individuals engaged in criminal activity like to keep instrumentalities, records, communications, and other evidence of their crimes in places where they can control access, and at places they believe will afford them the ability to keep these items concealed. These are often places where they can frequently be present to monitor the premises to ensure their activities will not be discovered. Some examples of such places would be on their persons, homes, storage units, or vehicles. Thus, the premises to be searched is consistent with these requirements.

58. In order to corroborate the owner of Attachment A (including any digital devices contained therein as described in Attachment B that belong to Marcos or Joy Trevino), as well as the identities and locations of potential co-conspirators, it will be necessary to review the contents of their emails and documents, as well as contextual information such as their address books, contact or buddy lists, bills, invoices, receipts, registration records, correspondence, notes, records, memoranda, telephone/address books, photographs, video recordings, audio recordings, lists of names, records of payment for access to other online subscription services, and attachments to emails, including documents, pictures and other files.]

59. Based on my training, my experience, and this investigation, I know that because of constantly expanding capacities, people tend to keep emails and other information such as attached files on their digital devices for long periods of time. This mirrors the fact that online service providers expressly encourage their subscribers to retain their emails and other information by offering increasingly larger email boxes and other services. Users often respond to these incentives by not deleting items from their accounts – or their digital devices.

Computers, Electronic Storage, and Forensic Analysis

60. As this investigation is being conducted by the FBI's Houston Field Office, Bryan Resident Agency, the FBI seeks to seize digital devices and for administrative convenience, bring them back to its facilities in Texas where it can conduct the searches there.

61. As described above and in Attachment B, this application seeks permission to search for records described in Attachment B that might be found at the place to be searched (Attachment A), in whatever form they are found that can be readily identified as being used by Marcos and/or Joy Trevino. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the

seizure of electronic storage media or, potentially, the copying of electronically stored information belonging to Marcos and/or Joy Trevino, all under Rule 41(e)(2)(B).

62. *Probable cause.* I submit that if a computer or storage medium belonging to Marcos and/or Joy Trevino is found at the place to be searched (Attachment A), there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from

operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

63. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files belonging to Marcos and/or Joy Trevino that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence belonging to Marcos and/or Joy Trevino that establishes how their computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on Marcos and/or Joy Trevino’s storage medium in the Place to be Searched (Attachment A) because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can

record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other

evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of

knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that in schemes similar to the one described in this affidavit, the target individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

64. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on

the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

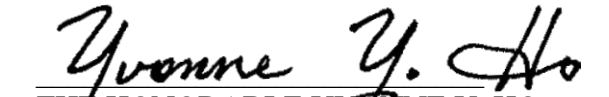
c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

65. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.



Jared Harshbarger
Special Agent, FBI

SWORN AND SUBSCRIBED to me by telephone on this 9th day of April,
2022, and I find probable cause.



THE HONORABLE YVONNE Y. HO
UNITED STATES MAGISTRATE JUDGE
Southern District of Texas

ATTACHMENT A

PROPERTY TO BE SEARCH AND DESCRIPTION OF PREMISES TO BE SEARCHED

This warrant applies to information associated with **MARCOS TREVINO** that is premises owned, maintained, controlled, or operated by **MARCOS TREVINO**.

Specifically, the residence located at 9418 Lancaster Drive, Iola, TX, 77861, as depicted in the picture below. This warrant also seeks authority to search any detached structures on the property, including, but not limited to, the garage.



ATTACHMENT B

Particular Things to be Seized

The following items to be seized in whatever form (including electronic), found at the Premises to be Searched described in the Attachment A, including any digital devices belonging to Marcos and/or Joy Trevino, for evidence, fruits or instrumentalities of violations of 18 U.S.C. § 1953, 1343, and 1349 (the “Subject Offenses”), as further described in the search warrant affidavit. These items are specifically described below and includes any of Marcos and/or Joy Trevino’s digital devices found at the Premises to be Searched described in Attachment A.

1. Information and items, regardless of date, of Marcos and/or Joy Trevino that may establish ownership and control (or the degree thereof) of the Place to be Searched (Attachment A), including address books, contact or buddy lists, bills, invoices, receipts, registration records, bills, correspondence, notes, records, memoranda, telephone/address books, photographs, video recordings, audio recordings, lists of names, records of payment for access to newsgroups or other online subscription services, and attachments to emails, including documents, pictures and files.

2. Safes, safety deposit boxes, keys for safety deposit boxes, hidden compartments, and other secure locations, which often contain the proceeds of Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349), including United States currency, as well as books and records regarding the acquisition, use, and disposition of such items.

3. The **Target Vehicle** and records relating to proof of ownership of the VIN: 2C3CDZH98JH102818 (“**Target Vehicle**”), any information regarding a lease, service information, lien, or any other information regarding the **Target Vehicle**.

4. Cellular phones, electronic devices, and electronic storage media devices capable of being read by a computer that belong to Marcos and/or Joy Trevino (which will be searched in

accordance with the attached Addendum), and/or proof of ownership or use of such phones or devices, including sales receipts, bills for internet access, and handwritten notes.

5. Records and information relating to the identity or location of any co-conspirators which may relate to the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

6. Records and information relating to potential victims related to the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

7. Bank statements, cards, transfer/withdrawal receipts or other financial records that may be involved in or evidence of the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

8. Information and items relating to the fraudulent scheme described in the affidavit that is related to the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

9. Information and items, regardless of date, relating to the identity, location, or role of any co-conspirator related to the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

10. Information and items, regardless of date, that would identify and locate persons who are victims or co-conspirators.

11. Computers or storage media that belong to Marcos and/or Joy Trevino used as a means to commit the violations described above that are related to the Subject Offense (18 U.S.C. §§ 1953, 1343 and 1349).

12. Information and items related to Marcos and/or Joy Trevino's digital devices that may have been used to commit the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

13. Information and items related to the proceeds fraudulent scheme described in the affidavit that is related to the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

14. Documents or records which identify the user of cell phone, electronic devices, and electronic storage media devices capable of being read by a computer (which will be searched in

accordance with the attached Addendum) that belong to or are in the possession (actual or constructive) of Marcos and/or Joy Trevino, and documents or records which identify who controls the cell phone, electronic devices, and electronic storage media devices, including contact lists, or, for phones belonging to or in the possession (actual or constructive) of Marcos and/or Joy Trevino, and other information located in the abovementioned phone or device's memory.

15. Information and items, regardless of date, that demonstrate the state of mind of the owner and users of the Place to be Searched (Attachment A), which would be Marcos and/or Joy Trevino, as well as that of other co-conspirators, with respect to the Subject Offenses (18 U.S.C. §§ 1953, 1343 and 1349).

16. Evidence or lack thereof such items which would be consistent with facilitating a vehicle raffle, such as promotional flyers, ledgers, "koozies", partnership with dealers, and involvement with car shows.

17. For computer or storage medium belonging to or in the possession (actual or constructive) of Marcos and/or Joy Trevino whose seizure is otherwise authorized by this warrant, and computer or storage medium belonging to or in the possession (actual or constructive) of Marcos and/or Joy Trevino that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind, intent and knowledge as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence such as hard drives, solid state drives, flash drives, CDs, DVDs, SD cards, magnetic tape, cameras, or other computers;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages,

search terms that the user entered into Internet search engines, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

n. routers, modems, and network equipment used to connect computers to the Internet.

The term “computer” as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. This term expressly includes items that fit this definition even if they are not commonly referred to as “computers.” Such items include smart phones and tablets. Unless otherwise indicated, “computer” is used interchangeably with “digital device.”

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

The terms “information,” “records,” “documents,” “programs,” “applications,” and “materials” include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the items described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the items described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
 - b. searching for and attempting to recover deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;
- and

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the items described in Attachment A within 180 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.